AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (currently amended) A method of making an electronic entity with encrypted access secure when said electronic entity executing a cryptographic algorithm consisting in applying to an input message a succession of groups of operations known as "rounds" involving a series of respective sub-keys produced successively by an iterative process starting from an initial key K, the method comprises performing steps of said iterative process so as to obtain a result of an ~~iterative~~ intermediate step,

storing in said electronic entity said result of said intermediate step,

repeating at least some of the steps of said iterative process until a result is recalculated corresponding to the result that has been stored,

comparing the value of said stored result to the value of the corresponding recalculated result, and

prohibiting the broadcasting of an encrypted message resulting from the application of said algorithm if said two values are different.

2. (previously presented) The method according to claim 1, further comprising:

storing a sub-key and repeating at least some of the steps of said iterative process until a sub-key is recalculated corresponding to said stored sub-key.

3. (previously presented) The method according to claim 1, further comprising:

storing the value of an intermediate result (R_m) of said iterative process and repeating at least a portion of said iterative process until an intermediate result is recalculated corresponding to the stored intermediate result.

4. (previously presented) The method according to claim 2, further comprising:

storing the value of the final sub-key (K_n) and repeating at least a final portion of the steps of producing the succession of said sub-keys until said final sub-key is calculated a second time.

5. (previously presented) The method according to claim 4, further comprising:

repeating all of the steps of producing the succession of said sub-keys.

6. (previously presented) The method according to claim 1, wherein the method is applied to an AES algorithm.

7. (previously presented) The method according to claim 1, wherein the method applied to a DES algorithm.

8. (previously presented) An autonomous electronic entity wherein it comprises means (13) for implementing the method according to claim 1.

9. (previously presented) An electronic entity according to claim 8, wherein it takes the form of a microcircuit card.